CPSC 454 Cloud Computing & Security

Course Overview

Instructor: Yun Tian

Course Information

- Instructor: Dr. Yun Tian
  - Office: CS 544
  - E-mail: ytian@fullerton.edu
  - Phone: (657) 278-2041 (office)
- Office hours
  - Mon. & Wen.: 3:00 PM to 4:00 PM
  - Tu. & Th.: 2:00 PM to 2:30 pm
  - Or by appointment

Course Information

- **Section 01**
  - Time: TuTh: 2:30PM - 3:45PM
  - Place: CS 110B - Lecture Room
- **Section 02**
  - Time: TuTh: 4:00PM - 5:15PM
  - Place: CS 102A - Lecture Room

3

Course Website

- TITANium
  - Grading
  - Schedule
  - Lecture notes
  - Discussion
  - Project submission
  - …

Prerequisites and Course Materials

- CPSC 333: Introductions to Computer Security
- CPSC 351: Operating System
- No text book.
- Lecture notes are provided. In addition, we also collect materials from the web.

Who should not take this course?

- I do not want to do programs (such as C, C++, java, web2.0, SQL, MySQL, etc.) and just want to learn cloud computing concepts.

6

Attendance

- Attending the lectures is mandatory--no textbook.
- Students are responsible for all course material regardless of whether they are present or absent.
- Attendance will be recorded from time to time.
- Two lateness or tardiness counts one absent.
- Students who are absent for 5 or more times will receive an "F" for this class.

7

Class Objectives

- The course is designed to introduce cloud computing and the related security techniques to CS curricula and provide students the fundamental background of cloud computing enabling technologies with hands-on experience. Student will
  1. learn the core concepts and principles of cloud computing and cloud security as well as identify and explore some of the emerging research challenges in cloud computing and cloud security;
  2. gain hands-on experience in using cloud computing infrastructure by designing, developing and deploying applications on cloud infrastructures; and
  3. work on a large research project in cloud computing.

Course Description

- The lecture materials will focus on the cloud computing models and applications, virtualization technologies, and different cloud security techniques.
- Through course projects, students will learn project design, management, implementation, testing and reporting skills.

Course Coverage Overview (1)

- Students will learn:
  - What is virtualization and Cloud computing and its history and evolution?
  - Architecture and models that support cloud computing service frameworks.
  - Resource (computing, storage, and network) virtualization
  - Cloud computing infrastructure requirements and limitations
  - Cloud Computing architecture and industry frameworks such as MapReduce (Hadoop)
  - Practical applications (virtual lab and mobile cloud computing)

10

Course Coverage Overview (2)

- Monitoring, management, and security protection of cloud computing
- Software networking and risk mitigation methodology for cloud computing.
- Vulnerabilities and risks of cloud computing
- Data classification and protection in cloud
- User identification and access control in cloud computing
- Open research issues in cloud computing and security
- Hands-on experience on cloud system establishment and building large-scale cloud computing applications

11

Recommended Readings

- Tom White, "Hadoop: The Definitive Guide", Second Edition, O'Reilly Media, 2010.
- James E. Smith, and Ravi Nair, Virtual Machines: Versatile Platforms for Systems and Processes, First Edition, Morgan Kaufmann, 2005.
- Jurg van Vilet and Flavia Paganell, "Programming Amazon EC2", O'Reilly Media, 2011.
- Jothy Rosenberg and Arthur Mateos, "The Cloud at Your Service", First Edition, Manning Publications, 2010.
- Sean Owen, Robin Anil, Ted Dunning and Ellen Friedman, "Mahout in Action", First Edition, Manning Publications, 2011.
- Chuck Lam, "Hadoop in Action", First Edition, Manning Publications, 2011.
- Internet, Google is your best friend!

Course Assignment

- There will be one assignment on the survey of a self-chosen cloud computing technical areas. (count for 20% of the overall grade)
- Further guidelines will be provided when the assignment is released.

Course Projects

- The project will count a combined total of 30% of your score. There are 3 project phases throughout the course.
  - The first phase is project proposal and plan, it is worth 5%.
  - The second phase is project midterm report. It is worth 10% including a presentation (5%) and a progress report (5%).
  - The third phase is the project final report and presentation. It is worth 15%, including a presentation (5%), a final report (5%), and demo (5%).

Expected Outcomes

- Students will explain the core concepts of the cloud computing paradigm: how and why this paradigm shift came about and the influence of several enabling technologies in cloud computing.
- Students will study the main security issues, challenges and the related techniques of cloud computing.
- Students will examine the process of working on a large research project. You will study how applications for clouds are written, deployed and analyzed. In the process, they will develop the needed skills to go through project planning, design, implementation, analysis and reporting.
- Students will identify some of the emerging cloud computing and the related security challenges.

Grading

- **Midterm Exam (20%).**
- **Final Exam (30%)**.
- **Term project (30%):** There will be a group project (at most 4 students) on a selected topic in the areas: cloud resource management/monitoring, cloud computing for big data, and cloud security. More details on the project topics will be discussed in the first four weeks of the semester.
- **Survey Paper (20%):** There will be one survey paper assignment on the survey of a self-chosen cloud computing and cloud security technical areas. This survey paper also includes a part of your study summary. More details of the survey paper will be discussed in the first four weeks of the semester.

Midterm Exam and Final Exam

- **Two exams are given.**
  - The first exam is given around the eighth or ninth week
  - Final Exam
    - o Section 01
      Thursday, December 14, 2:30 - 4:20 pm @ CS 110B
    - o Section 02
      Tuesday, December 12, 5:00 - 6:50 pm @ CS 102A
  - Make up exam is permitted, if the student calls me one week before the exam is given.

Submission Policy

- Late submission will downgrade your project grade (10% per day).
- Late submission after 24 hours will not be accepted.

Attendance

- Attending the lectures is mandatory. Students are responsible for all course material regardless of whether they are present or absent.
  - If you must be absent on a day when submissions are due, you must make special arrangements to turn in your submission ahead of time.
  - These arrangements must be made at least two business days ahead of the deadline.
  - Participate in class discussions (don't be afraid)!
  - Take part in the online class discussion forum on TITANium

Class Policies

- Cheating
  - Cheating is a serious problem!!!
- Laptop in class
  - Laptop is allowed in the back rows of the classroom.
- Late in class
  - If you are late 30 minutes after the class starts, please do not enter the classroom.

20

Collaboration Policies

- You are required to compose your own unique solution to each problem and each project.
- Some obvious acts of cheating are:
  - turning in work done by someone else
  - copying work done by someone else

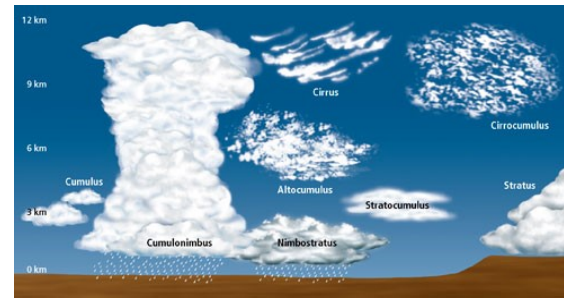
  We have no problem failing you in this class for the semester and having the appropriate entries placed in your student records.
- **I will be using a cheating detection software to compare all students files.**

Questions ?

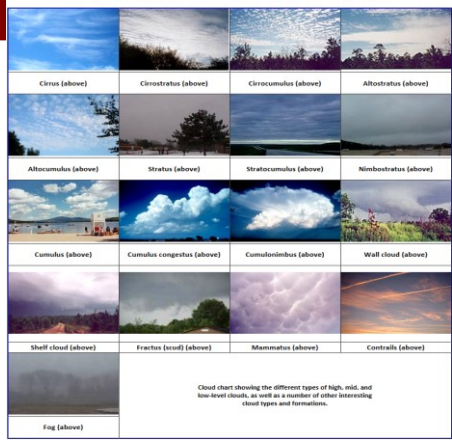
Definition of Cloud Computing

23

Cloud Classification



24



25

NIST Definition of Cloud Computing

- NIST(National Institute of Standards and Technology) Special Publication 800-145http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model is composed of **five** essential characteristics, **three** service models, and **four** deployment models.

26

Five Essential Characteristics

1. **On-demand self-service**.

   A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

27

Five Essential Characteristics

2. **Broad network access**.

   Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

28

Five Essential Characteristics

3. **Resource pooling**.

   The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

29

Five Essential Characteristics

4. **Rapid elasticity**. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

30

Five Essential Characteristics

5. **Measured Service**.
Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

*Typically this is done on a pay-per-use or charge-per-use basis.

31

Three Service Models

1. **Cloud Software as a Service (SaaS)**

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure*. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

32

Three Service Models

2. **Cloud Platform as a Service (PaaS)**.

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider*. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

*This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

33

Three Service Models

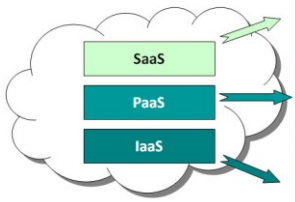
3. **Cloud Infrastructure as a Service (IaaS)**.

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

34

Cloud Computing - Services

Software as a Service - SaaS
Platform as a Service - PaaS
Infrastructure as a Service - IaaS



Who Uses It	What Services are available	Why use it?
Business Users	EMail, Office Automation, CRM, Website Testing, Wiki, Blog, Virtual Desktop ...	To complete business tasks
Developers and Deployers	Service and application test, development, integration and deployment	Create or deploy applications and services for users
System Managers	Virtual machines, operating systems, message queues, networks, storage, CPU, memory, backup services	Create platforms for service and application test, development, integration and deployment

35

Four Development Models

1. **Private cloud**.

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

36

Four Development Models

2. **Community cloud**.
   The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

37

Four Development Models

3. **Public cloud**.

   The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

38

Four Development Models

4. **Hybrid cloud**.
   The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

39

Summary

- Five essential characteristics: On-demand self-service; Broad network access; Resource pooling; Rapid elasticity; and Measured Service.
- Three service models: Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS).
- Four deployment models: Private cloud; Community cloud; Public cloud; and Hybrid cloud.
- Is this definition sufficient?

40

What you need to do this week?

- Read Intel guide of how to build a cloud system and get familiar with cloud virtualization system.
- Resource can be found at the TITANium
- Get to know each other and compose group partners
  - Use TITANium's discussion board to share your thoughts and search for project partners
- Investigate project topics